SECTION 1. GENERAL PROVISIONS

Part 1. INTRODUCTION

'1-100 Objective. The security of the U.S. depends in part on the proper safeguarding of classified information released to industry. The objective of the DoD Industrial Security Program is to assure the safeguarding of classified information in the hands of U.S. industrial organizations, educational institutions, and all organizations and facilities used by prime and subcontractors, hereinafter referred to as industry. The objective of this regulation is to set forth policies, practices, and procedures of the DoD Industrial Security Program used internally by the DoD to ensure maximum uniformity and effectiveness in its application throughout industry. The ISM, as a companion document to this regulation, is a DoD publication which contains detailed security requirements to be followed by U.S. contractors for safeguarding classified information. The ISM is made applicable to industry by execution of the "DoD Security Agreement" (DD Form 441), and by direct reference in the "Security Requirements Clause" in the contract. Should * there develop any conflict in instructions between the ISM and this regulation, such conflict shall be reported to the Director, Defense Investigative Service (DIS), ATTN: Deputy Director (Industrial Security). . _ Pending resolution, the provisions of this regulation shall govern.

1-101 Authority and Scope. This regulation, authorized by the Secretary of Defense under the authority of the National Security Act of 1947, as mended, is established as a DoD regulation published by Headquarters (HQ) DIS under the authority of DoD Directive 5220.22, "DoD Industrial Security Program."

a. This regulation is applicable to the OSD (including all of its boards, councils, staffs, and commands), DoD agencies, and the Departments of the Army, Navy, and Air Force (including all of their activities), hereinafter referred to as User Agencies (UA's), in all industrial security relationships with industry.

b. The Secretary of Defense is authorized to act on behalf of the UA'S listed in paragraph 1-273.

c. The DIS shall administer the DoD Industrial Security Program on behalf of all UA's.

(1) The Regional Directors of DIS have the authority and responsibility for administration of the DoD Industrial Security Program within their respective regions. The offices of the Directors of Industrial Security are designated as the cognizant security offices (CSO's) for all contractor facilities within their jurisdictions and are responsible for the performance of CSO functions prescribed in this regulation, except for certain security actions noted elsewhere herein which may be performed by the Commander or Head of a UA installation or the Regional Directors of DIS. Facility security clearances (FCL's) shall be granted by the CSO.

(2) The Director, Defense Industrial Security Clearance Office (DISCO), DIS, Columbus, Ohio 43216, shall assume responsibility for processing and granting all industrial personnel security clearances (PCL's) (except for contractor-granted CONFIDENTIAL clearances), including those PCL's for contractor personnel located on a UA installation, and for maintaining an industrial personnel security clearance file (PSCF) of PCL's and FCL's.

(3) UA's have the authority and exercise the functions of, a contracting activity as prescribed in this regulation and the ISM. Certain of these functions, under the delegation of the PCO are performed by the ACO (see appendix C).

d. This regulation implements the security policies established by the Deputy Under Secretary of Defense for Policy (DUSD(P)) and establishes the procedures, requirements, and practices concerned with the effective protection of classified information in the hands of industry, including foreign classified information which the U.S. Government is obliged to protect, in the interest of national security. UA'S are not authorized to require a different standard of industrial security than prescribed herein, except as authorized in paragraph 1-114. In addition, this regulation implements the DoD Operations Security (OPSEC) Program established by DUSD(P) as set forth in DoD Directive 5205.2, "DoD Operations Security Program." Section X of this regulation provides amplifying and procedural guidance for UA's when considering Imposition of OPSEC requirements on industry.

(1) This regulation is. written in terms of the most common situation where the contractor has access to, or possession of, classified information in connection with the performance of a classified contract. However, it is also applicable to the safeguarding of classified information in connection with all aspects of precontract activity, including preparation of bids and proposals and precontract negotiations, and all aspects of postcontract activity. Moreover, the requirements are equally applicable to the safeguarding of classified information not released or disclosed under a procurement contract such as U.S. Government-sponsored independent research and development advance agreements *or* UA programs participated in by a firm, organization, or individual on a voluntary or grant basis. Examples of the latter programs are long-range scientific and technical planning programs and programs designed to provide planning briefings for industry. Contractors participating in such programs shall be advised of the following: "The recipient shall safeguard all classified material and shall provide and maintain a system of security controls within its organization in accordance with the requirements of: (i) the 'Department of Defense Security Agreement' (DD Form 441), (ii) "the ISM (attachment to DD Form 441), and (iii) any revisions or changes to the ISM required by the demands of national security as determined by the U.S. Government." In such situations, the official of the UA, or designee, who releases or discloses the classified. information to the firm, organization, or individual shall fulfill the responsibilities which this regulation and the ISM assign to the contracting officer (such as, furnishing necessary classification guidance, authorizing retention of classified material, and certifying contractors' need-to attend classified meetings).

(2) When foreign classified information is made available to a contractor-by a UA in connection with a U.S. classified contract, procedures applicable to U.S. classified information shall be used. However, when foreign classified information is made available to U.S. contractors in connection with a foreign classified contract, the responsibility for the actions which this regulation and the ISM charge to the contracting officer and the contracting UA shall be as prescribed in paragraph **8-103e. Responsibilities** not specifically

, assigned in paragraph 8-103. are reserved to the foreign government agency or foreign contracting activity concerned.

(3) When a report-is submitted in accordance with paragraph 6a (18), ISM, the CSO shall contact the originator, or, where appropriate, the authority releasing the classified material to the contractor to: (i) identify the source and contact for obtaining classification guidance relating to the material, (ii) establish the contractor's need for the material, (iii) determine the safeguards that are prescribed for the protection of the material, and (iv) determine the disposition instructions which are applicable to the material. Upon receipt of the classification guidance and disposition instructions from the releasing authority, the CSO shall provide such information to the contractor. UA's originating such material, or releasing or authorizing the release of such material to contractors, shall assist CSO's in establishing appropriate guidance and instruction for contractors who receive classified material without proper guidance for its protection and disposition.

e. Any situation or emergency which indicates a need for clarification, modification, addition, or deletion to this regulation shall be reported promptly, together with recommendations, through channels to the DIS, ATTN: Deputy Director (Industrial Security). Temporary action is authorized to be taken by a' UA to safeguard its classified information in an emergency situation.

f. This regulation shall not be construed to limit in any manner the authority of the. Secretary of Defense, the Secretaries of the Army, Navy, and Air Force, or the Heads of UA'S individually; to grant access to classified information under the cognizance of their department or agency, to any individual designated by them. The granting of such access is beyond the scope of the DoD industrial Security Program.

g. The Deputy Director (Industrial Security), HQ DIS is responsible for the implementation and administration of security procedures applicable to the transmission of SECRET material by commercial carriers.

h. The Commander, Military Traffic Management Command (MTMC) is responsible for the Implementation and administration of security procedures applicable to the transmission of CONFIDENTIAL material by commercial carriers within the continental U.S. (CONUS). Designated Commanders will provide this service in prescribed areas outside the CONUS (also see appendix F). .

i. All U.S. Arms Control Disarmament Agency" (ACDA) contracts involving contractor access to RESTRICTED DATA are, by separate agreement between ACDA and the Department of Energy (DOE), the responsibility of the DOE.

1-102 Superseded Regulation. This regulation supersedes the ISR dated February 1984 and Changes thereto. *

1-103 Responsibilities. "Security responsibility for contracts awarded to industry is set forth below (see section VIII for contracts awarded to foreign industry).

a. The contractor is required to comply with the security provisions of the ISM and *with* any additional security requirements established by the contract, regardless of the geographical location of the classified material.

b. Within the U.S., Puerto Rico, or a U.S. possession or trust territory, the Deputy Director (Industrial Security) shall assume security cognizance for all contractor facilities within the region, and shall perform CSO functions prescribed in this regulation on behalf of all UA'S with respect to all contractor facilities within the region. However, in the case of contractor facilities located on a UA installation, certain security actions may be performed by the Commander or Head of the installation concerned (see paragraph 1-108). The Director of Industrial Security, Pacific Region, is assigned security cognizance for contractor 'facilities performing in U.S. trust territories or possessions in the Pacific area, and the Director of Industrial Security, Southeastern Region, is assigned security cognizance for contractor facilities performing in Puerto Rico, and U.S. possessions in the Atlantic and Caribbean areas. The appropriate CSO may make the necessary arrangements with the Commander or Head of the UA installation located closest to the contractor's operations to perform industrial security supervision and inspections of such operations on his or her behalf. Upon completion of the arrangement, the CSO will notify the HQ activity of the UA installation involved and the Deputy Director (Industrial Security,) HQ DIS as to the identity and the location of the Commander or activity performing the required industrial security supervision. If the above arrangements are not feasible, a security representative from the appropriate CSO shall make the required security inspections. The frequency of such inspections may be modified with the approval of the Deputy Director (Industrial Security), HQ DIS.

c. Outside the areas enumerated in paragraph b above, the UA awarding the classified contract shall assume responsibility for all security aspects of contract supervision (see paragraph 1-115) unless the UA requests this responsibility be undertaken by DIS.

d. The Director, DISCO shall assume responsibility for all industrial PCL functions prescribed by this regulation. Except in cases pertaining to owners, officers, directors, partners, regents, trustees, or executive personnel (OODEPs) which are transmitted through the CSO, contractors deal directly with DISCO on all PCL's, transfers of PCL's, and issuances of security assurances. The DISCO shall:

(1) process and issue PCL's for contractor personnel, including those employees located on UA installations;

(2) maintain the PSCF of contractor FCL's and PCL's;

(3) on request, furnish PCL information on contractor employees, including those on UA installations;

(4) on application by a U.S. contractor, make a security assurance determination predicated upon a LOC; and

(5) advise the Commander or Head of a User Agency installation whenever the security clearance for a contractor employee, who is duty stationed with a contractor activity on his/her installation, has been suspended, denied or revoked.

e. When shipping SECRET material by commercial carrier, UA's are responsible for obtaining the necessary routing instructions from MTMC, and for utilizing a carrier which has been qualified by MTMC and has been granted an appropriate FCL by the CSO. The MTMC, In turn, shall be responsible for assuring that a qualified carrier which has been granted an appropriate FCL by the CSO is used 1/, except where use of prepaid commercial bill of lading (CBL) has been authorized in the appropriate contract or approved by the contracting officer concerned 2/. SECRET material shall be shipped by government bill of lading (GBL) or CBL annotated thereon: "To be converted to a Government Bill of Lading." In addition, the notation, "Protective Security Service Required," shall be reflected on all copies of the bill of lading (BL). An annotated CBL must be converted to a GBL before payment is made. The BL's will be maintained in a suspense file to follow up on overdue or delayed shipments.

1-104 Arrangement of Regulation. This regulation covers the essential policies and procedures with respect to safeguarding classified information. It is divided into sections, parts, and paragraphs. Each section is designated by subject and Roman numerals (for example, I, II, and III), and covers a separate aspects of industrial security. The parts are designated by title and Arabic numerals (for example, 1, 2, 3), and contain a breakdown of the subject covered by the section into related divisions. The paragraphs are a further division of the parts. They are so numbered that the first digit indicates the section; the second digit, the part; and the last two digits, the paragraph (for example, 2-103, designates section II, part 1, paragraph 3; 3-314 designates section III, part 3, paragraph 14). The regulation is designed to permit subsequent insertions of additional parts and paragraphs within the appropriate section.

1-105 Amendment of Regulation. This regulation will be amended from time to time. Unless otherwise specified in any amendment, compliance with an amendment shall not be mandatory until 30 days after date of publication, although compliance shall be authorized from the date of its publication.

1-106 Distribution and Use of Regulation. This regulation is intended for the use and guidance of industrial security axial procurement 'activities of the UA's. It shall be distributed through normal channels to staff and operating activities concerned with industrial security and procurement matters. This regulation is not applicable to industrial management, and is not intended for distribution to industry. Parts or all of this regulation may be made available to industrial management, when judged to be in the interest of a UA .

1/ Non-DoD UA's may issue their own routing instructions; however, when doing so they will ensure that only commercial carriers which have been qualified by MTMC and granted an appropriate FCL by the CSO are utilized.

2/ In such cases, the SECRET shipment shall be routed via a cleared commercial carrier under a tariff, tender, or contract that provides PSS in accordance with DoD 5220.22-C (reference (b)).

1-107 User Agency Procedures Under This Regulation. UA's may augment this regulation by prescribing more detailed regulations and operating instructions as may be required and which are not inconsistent with this regulation. The application of these procedures shall be guided by the twofold objective of establishing uniformity and maintaining maximum security., consistent with the accomplishment by each UA of its assigned mission. Two copies of each implementing regulation or instruction issued by a UA shall be furnished to Director, DIS, ATTN: Deputy Director (Industrial Security) for information.

1-108 Contractor Activities on a User Agency Installation.

a. The Commander or Head of a UA installation shall provide security supervision of contractors and their employees located on the installation as follows .

(1) For installations located outside of the U.S., Puerto Rico, or a U.S. possession or trust territory, the contractor and his or her employees shall be considered to be visitors. In such cases the procedures set forth in paragraph e below shall apply.

(2) For installations located within the U.S., Puerto Rico, or a U.S. possession or trust territory, the contractor and his or her employees shall be considered to be visitors, or the Commander or Head of the installation may elect to declare the contractor activity a facility under one of the following criteria if:

(a) the contractor's operation is sufficiently complex to warrant assignment of an area such as a suite of offices, a building or portion thereof, or a segregated work area;

(b) the contractor's operation is to be of a quasi-permanent nature;

(c) the contractor maintains management control over his or her operations; or

(d) the contractor is in a position to maintain separate security procedures.

FCL's shall not be established on the installation solely for the purpose of permitting a contractor entry authorization into a controlled area unless access to classified information is required in the performance of the contract.

b. If, in light of the foregoing, the Commander or Head of the UA installation decides that the contractor's on-installation activity requires a FCL, he or she shall request the CSO in whose geographical area the installation is located (see appendix B for listing of CSO's and boundaries) to assume security cognizance of the facility. The Commander or Head of the installation shall request the CSO to perform all cognizant security functions provided for in this regulation, or he or she shall notify the CSO in writing that he or she has elected to perform the following security actions.

(1) Accomplish the FCL survey and furnish the CSO a copy of the "Facility Security Clearance -Survey" (DD Form 374), the DD Form 441 or the "Appendage to Department of Defense Security Agreement" (DD Form 441-1), the "Certificate Pertaining to Foreign Interests " (DD Form 441s), and exclusion certificates, as required.

(2) Assure that the contractor has prepared a standard practice procedure (SPP) , covering the contractor's operations on the UA installation.

(3) Assure that the contractor observes . required security controls through periodic inspections in accordance with the schedulé prescribed by paragraph 4-103, and furnish to contractors letters of requirements resulting from such inspections, if appropriate.

(4) Assure that the contractor maintains management control over his or her operations.

(5) Assure that prompt remedial action is taken where security conditions are deficient in the contractor's operations.

(6) Review, when appropriate, contractor control of incoming visitors to contractor facilities on the installation.

(7) Ensure that the DoD security education program is implemented by the contractor and, as required, conduct defensive security briefings required by paragraph 5U' ISM.

(8) Conduct investigation of contractor security violations, including loss, compromise, or suspected compromise of classified information in accordance with section V. If the services of a governmental investigative agency are required, request services from the appropriate military investigative agency.

(9) Furnish to the facility, guidance on the application of security requirements including establishment or disestablishment of closed or restricted areas. Requests from the contractor for interpretations of the requirements of the ISM shall be forwarded to the CSO.

(10) Request from DISCO interim PCL's for contractor personnel when required to prevent crucial delay in the negotiations or performance of the contract.

(11) Assure that the contractor reports promptly to the CSO and the Commander or Head of the UA installation any incidents which involve espionage, sabotage, subversive activity, or the loss, compromise, or suspected compromise of classified information.

(12) Recommend to the CSO the termination, revocation, or suspension of the FCL, as appropriate.

(13) Conduct the briefing and debriefing of the facility * security supervisor (FSO), the COMSEC custodian, and alternate COMSEC cus- *

todian when there is a COMSEC account or there is a requirement to establish a COMSEC account (see paragraph 2-313). Brief and debrief only the FSO if no COMSEC account is required.

c. When the security actions outlined in paragraph b above are performed by the Commander or Head of the installation, the following actions shall be accomplished by the CSO.

(1) Grant the FCL to the contractor provided the preclearance survey has been completed and the required fores are in order.

(2) Assign an industrial security specialist to accompany the installation security inspector during special or scheduled inspections upon request or as otherwise appropriate after coordination with the Commander or Head of the UA installation.

(3) Verify FCL and safeguarding ability, when requested (see paragraph 1-110b).

(4) Terminate, revoke, or suspend FCL's, as appropriate.

d. Reports of initial "Facility Security Clearance Survey," recurring inspections reported on "Industrial Security Inspection Report" (DD Form 696), letters of requirements to the contractor, and reports resulting from investigations conducted in accordance with section V shall be exchanged between the Commander or Head of the UA installation and the CSO.

e. If the Commander or Head of the UA installation does not elect to clear contractors on his or her installation as facilities, he or she shall provide appropriate security supervision and shall be responsible for the following:

(1) Provide written instructions specifying: (i) those security actions which will be performed for the contractor by the installation such as providing storage facilities, guard service, mail and freight services, and visit control, and (ii) those security actions for which joint action may be required such as the packaging and addressing of classified transmittals, and control of visitors.

(2) Ensure that the contractor-has prepared a SPP covering the contractor's activities on the UA installation," -if appropriate.

(3) Ensure that the contractor observes required security controls through periodic inspections in accordance with the schedule prescribed by paragraph 4-103, and furnish to contractors letters of requirements resulting from such inspections, if appropriate.

(4) Ensure that prompt remedial action is taken when security conditions are deficient in the contractor's operation.

(5) Ensure that the DoD security education program is implemented by contractors and, as required, conduct defensive security briefings required by paragraph 5u, ISM.

'(6) Conduct investigation of contractor security violations, including loss, compromise, or suspected compromise of classified information.

(7) Conduct the briefing and debriefing of the FSO, the COMSEC custodian, and alternate COMSEC custodian when there is a COMSEC account or there is a requirement to establish a COMSEC account (see paragraph 2-313). Brief and debrief only the FSO if no COMSEC account Is required.

(8) Furnish to the contractor guidance on the application of security requirements to the contractor's operations.

(9) Forward requests from the contractor for interpretations of the ISM to the CSO.

(10) Request from DISCO Interim PCL's for contractor personnel, when required, to prevent crucial delay in the performance of the contract.

(11) Ensure that the contractor reports promptly any incidents which involve espionage, sabotage, subversive activity, or the loss, compromise, or suspected compromise of classified information. In addition, the CSO of the visiting contractor's facility shall be advised concerning the incident.

f. For those installations located outside of the U.S., Puerto Rico, or a U.S. possession or trust 'territory, where the Commander or Head of the UA Installation has relinquished security responsibilities to DIS, the Office of Industrial Security International (OISI) and/or the appropriate CSO will be responsible for assuring that the security actions outlined in paragraph 1-108e above are accomplished.

1-109 Expenditure of Funds for Security. The CSO shall not commit the government to reimburse the management of *a* facility for funds expended in connection with the facility's security program. In the case of a cost-reimbursement-type contract, the allowability of security costs is determined by the contracting officer in accordance with the terms of the contract and with the cost principles of the Federal Acquisition Regulation (FAR) (reference (gg)). Under a fixed price contract, the initial contract price includes all applicable security costs. An equitable adjustment may be made in the initial contract price when, as indicated in the contract security clause, the security classification or security requirements under the contract are changed by the government and the change results in an increase or decrease in the contract price.

1-110 Disclosure of Classified Information to a Contractor by User Agency Contracting Activities.

a. Prior to the disclosure of any classified information to a facility, the contracting activity of the UA shall determine that the contractor's facility has a valid FCL equal to, or higher than, the category of classified information to be disclosed. If the facility will be required to have physical possession of classified material, the contracting activity shall also determine that the facility has the ability to properly safeguard the classified information to be disclosed. to, or developed by, the facility.

(This determination may be made at the same time as the FCL verification.) Such determinations shall be based on:

(1) the contracting activity's knowledge of the ability of the facility to adequately safeguard the material to be developed or released, based upon a current contractual relationship involving classified material of the same or higher category as that to be released or developed under the new contract or program; or

(2) the written verification by the Personnel Investigations Center (PIC) - Central Verifications Activity (CVA), 3/ mailing address:

Defense Investigative Service
PIC-CVA
P.O. Box 1211
Baltimore, MD 21203-1211
Telephone Number: (301) 633-4820

or the CSO if appropriate, of the safeguarding ability of the facility in the event that the procuring contracting activity does not have the knowledge required in paragraph (1) above. In this connection, the contracting activity shall furnish to the PIC-CVA or CSO of the facility information available (description, quantity, end item, and classification of the information related to the proposed contract or program, and any other facts) to assist the PIC-CVA or CSO in making such a determination.

b. The PIC-CVA, or the CSO if appropriate, shall furnish written verification to the contracting activity as to whether a facility has an appropriate FCL and has the appropriate safeguarding capability for the classified material involved. Unless otherwise notified (superseded) in writing by the PIC-CVA or CSO, each verification furnished In accordance with this paragraph shall remain valid for a period of 1 calendar year from the date of issuance. In the event a FCL has not been issued, the requester shall be so advised. Further action shall not be taken unless a formal request to clear the facility is received by the CSO.

c. The verification of safeguarding ability furnished by the PIC-CVA or CSO shall be based upon inspections conducted in accordance with this regulation, or in the event the facility is not on the current inspection schedule, upon a visit which has been made to the facility to obtain the required data. Written verification shall be dispatched within 5 working days from receipt of inquiry.

3/ Under the following circumstances, the PIC-CVA will not be able to respond and requesters shall make inquiries to the appropriate CSO: (i) requests involving the transfer, of material that would require more than two cubic feet of storage, (ii) requests involving commercial carriers under the-provision of paragraph 17c(5)(c), Industrial Security Manual, and (iii) requests for certification of security clearance and safeguarding ability to the Defense Technical Information Center.

d. In the event the FCL must be revalidated or raised to an appropriate level, or the f acility must provide adequate safeguards in order to comply with the requirements of- the ISM, the requester shall contact the * CSO which will advise them of the nature of such actions, and of the esti- * mated time required to complete such actions. Moreover, the requester shall be asked to advise as to whether the CSO should initiate action to have the FCL revalidated or raised to an appropriate level. Additional action shall not be taken by the CSO unless the requester advises that it is necessary * to bring the FCL to a valid status. In such cases, appropriate action shall be initiated promptly by the CSO and the requester shall be informed when action is completed.

e. When noncontract-related classified material is released under a Scientific and Technical Information Release Program, or a classified contract is awarded which requires classified reports *to* be disseminated to other individuals or firma in accordance with a standard mailing or distribution list, the sponsoring, releasing, or contracting activity, as appropriate, has the following responsibilities in' order to make certain the intended recipients are eligible to receive the classified information.

(1) Verify initially the need-to-know, FCL, and safeguarding capability of the recipients of the reports, unless this requirement is levied on the prime contractor.

(2) Ensure that the recipients of classified material are provided appropriate classification guidance and instructions, to assure proper identification, control, accountability, handling, protection, and ultimate disposition of classified information, to include specific retention authority, which the individual or company may be required to use in its operations and for discussions involving classified information.

(3) Notify appropriate PIC-CVA, *or* appropriate CSO(s), if * applicable, and the prime contractor of any change in the mailing list. *

(4) Require in the contract or other appropriate written notification that the releasing activity or the prime contractor making the distribution of the reports determines the storage and safeguarding capability of the recipient from the PIC-CVA, or appropriate CSO, if applicable, * prior to making the first release of any reports. Subsequent releases of material may be made without reverification of storage and safeguarding ability until such time as the distribution list is revised to delete the recipient.

f. The FCL verification notification shall be retained for one * year, after which it shall be destroyed. The recipient of the verification * notification shall be immediately notified should a change occur adversely affecting the level of-the FCL *or* the safeguarding ability of the facility.

g. The DISCO shall not verify FCL's or safeguarding ability. This information shall be obtained from the PIC-CVA or the CSO of the * facility, if applicable. *

1-111 **Disclosure of Classified Information to a Subcontractor by a Prime Contractor.**

a. Prior to the disclosure of any classified information to a subcontractor, the prime contractor shall determine that the subcontractor has a valid FCL equal to or higher than the category of classified information to be disclosed, unless there is an existing contractual relationship between the parties involving classified information of the same or higher category as that to be released or developed under the new subcontract. A prime contractor, having verified a prospective subcontractor's FCL, shall obtain the written approval of the contracting office of the prime contract concerned, prior to disclosure of TOP SECRET information 4/ to the prospective subcontractor. *

b. If the prospective subcontractor will be required to have physical possession of TOP SECRET, SECRET, or CONFIDENTIAL material during the precontract or performance stages of the classified subcontract, the prime contractor shall, in addition to verifying the subcontractor's FCL, also determine that the subcontractor has the ability to safeguard properly the classified information to be released or developed under the subcontract. Such determination shall be based on:

(1) the prime contractor's knowledge of the ability of the prospective subcontractor to safeguard adequately the material to be released and produced, based upon a current contractual relationship involving classified material of the same or higher category as that to be released or developed under the new subcontract, or

(2) the written verification from the PIC-CVA, or the CSO * if appropriate, of the safeguarding ability of the prospective subcontractor, in the event the prime contractor does not have the knowledge required in paragraph (1) above. In this connection, the prime contractor shall furnish the PIC-CVA or if appropriate, the CSO of the prospective subcontractor * information available to him or her (such as description, quantity, end item, and classification of the information related to the proposed subcontract., and any other facts) in order to assist the PIC-CVA or CSO in making such a * determination. ,

---

4/ A contractor is not authorized to release classified intelligence information to a subcontractor, vendor, or supplier without proper written authorization of the contracting UA. All classified intelligence information, whether obtained during a visit or through other sources, shall be safeguarded and controlled in accordance with the provisions of the ISM, with any additional instructions which may be received from the releasing UA activity and any specific restrictive markings or limitations appearing on documents. All inquiries concerning source, acquisition, use, control, or restrictions pertaining to intelligence information shall be directed to the contracting UA activity concerned. This activity shall either handle the inquiry or arrange with other authorized releasing activities within the UA to handle the inquiry and provide guidance as requested. *

(3) The PIC-CVA, or the CSO if appropriate, shall advise * the requesting prime contractor of the current FCL status and safeguarding ability of the prospective-subcontractor as prescribed in paragraphs 1-110C, d, e, and f.

1-111.1 Disclosure of Critical Nuclear Weapon Design Information (CNWDI).

a. Prime Contractors. When a contracting officer has a requirement to release CNWDI information to a contractor, the CSO will be so advised and requested to brief the FSO and his or her alternate. In addition to the other requirements established for the release of classified information to contractors, CNWDI shall not be released unless the FSO and his or her alternate have been briefed by the CSO. The briefing shall include the definition of CNWDI, a reminder as to the extreme sensitivity of the information, and an explanation of the individual's continuing responsibility for properly safeguarding CNWDI and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a specific need-to-know for the particular information. The CSO shall maintain a record stating that the FSO and his or her alternate have been briefed and that the facility is authorized for access to CNWDI. Verification of the facility's eligibility for access to CNWDI may be obtained from the PIC-CVA, or the CSO if appropriate, or the * determination of the facility's eligibility may be based on the contracting activity's knowledge based upon a current classified contract with the contractor involving access to CNWDI.

b. Subcontractors. Contracting officers shall authorize prime contractors to release CNWDI to subcontractors, only after it has been determined that the subcontractor FSO and his or her alternate have been briefed as required in paragraph a above. The CSO shall also maintain a record that the facility is authorized access" to CNWDI in the same manner as provided in paragraph a above. Similarly, verification of the facility's eligibility for access to CNWDI may be verified through the PIC-CVA, or the CSO if appropriate, or * based upon a current classified contract with the subcontractor involving access to CNWDI.

c. Consultants. Type A Consultants may be briefed and afforded access to CNWDI, but such access may be permitted only at the facility of the contractor who engaged the Type A Consultant or at the government contracting activity. Type B and C Consultants shall not be briefed or afforded access to CNWDI without the prior approval of the contracting officer.

1-112 Applicability to Subcontractors and Their Employees. The procedures established in this regulation pertaining to contractors and their employees are equally applicable to subcontractors, vendors, or suppliers and their employees and, in turn, to each succeeding tier of subcontractors. Each subcontractor will be regarded by the DoD to be in the same category as a prime contractor with respect to his or her individual subcontractors.

1-113 Public Disclosure. In-accordance with paragraph 50, ISM, * contractors are precluded from releasing, for public dissemination, * Information pertaining to classified contracts or programs, except after * approval by the Directorate for Security Review, Office of the Assistant *

Secretary of Defense (Public Aff airs) (OASD (PA)) .5/ In the review for approval for public release, a determination must be made to ensure: (i) that classified inf ormat ion is not contained in the proposed release, (ii) that unclassified information which might not be in the national interest, such as militarily critical technology, is not revealed in the proposed release, and (iii) that the limitations and policies governing unclassified technical data under the International Traffic in Anus Regulation (ITAR) or the Export Administration Regulations (EAR) 6/ are adhered to .7/ DoD Directive 5230.9 (reference (d)), establishes policies and procedures, and assigns responsibilities governing the review and clearance of information proposed for public release by DoD.

a. DoD 5230.9 directs, inter alia, that information for public release shall be submitted to OASD(PA) for review and clearance prior to disclosure if the information:

(1) originates or is proposed for publication or release at the Seat of Government; or

(2) meets any of the following criteria:

(a) is or has the potential to become an item of national or international interest or has foreign policy or foreign relations implications;

(b) concerns high level military or DoD policy or U.S. Government policy;

(c) concerns subjects of potential controversy among DoD Components or with other federal agencies;

(d) concerns the following subject areas:

5/ If the information pertains to a classified contract or program awarded by a non-DoD agency, requests for approval for release shall be submitted to that non-DoD agency.

6/ Part 379 of the Export Administration Regulations and Section 125 of the International Traffic in Arms Regulation, are applicable.

7/ Release of unclassified technical data is governed by the Export Administration Act of 1979, administered by the Department of Commerce, and the Arms Export Control Act of 1976, administered by the Department of State through the International Traffic in Arms Regulation. After information is reviewed for security and determined to be unclassified, a further determination must be made for compliance with the export laws and regulations before it is finally approved for public release. This review is necessary because approval for public release may negate the requirement to obtain an export license for that information.

1. new weapons *or* weapons systems of significant modifications or improvements to existing weapons or systems, equipment, or techniques;

2. military operations, operations security, potential operations, and significant exercises;

3. national command authorities and command posts;

4. military applications in space, nuclear weapons, including nuclear weapons effects research, chemical warfare, defensive biological and toxin research, and high energy lasers and particle beam technology;

5. material involving critical military technology (see paragraph 1.221.2);

6. communications security, signals intelligence, and computer security; and

7. others as the OASD(PA) may designate.

b. Heads of DoD Components have clearance authority for, information not specified in paragraph-a above, and may delegate this authority to the lowest echelon competent to evaluate the content and implications of the information. Reviewing officials in the User Agencies. must understand their responsibility for identifying the information specified in paragraph a above, which must be reviewed by higher authority to determine its releasability. User Agencies should refer all doubtful cases to higher authority or to OASD(PA) for resolution.

c. It is the policy of the DoD that the university community, engaged in classified research work, be permitted to publish with minimum delay, the unclassified results of such research. To ensure the expeditious processing of such information, no delay of more than 30 days shall elapse from date of receipt without dispatch of an explanatory communication to the submitting college or university by the reviewing command or other authority. Denial of clearance of an entire paper or other material should be avoided when it is possible to approve clearance, with amendments, to eliminate identified security information.

1-114 Waivers, Special. Access Programs, and Carve-Outs.

a. The DUSD(P), his or her designee, or higher authority, shall provide overall policy guidance to this program and shall approve waivers to, or deviations from, the DoD security policy promulgated *in* this regulation and in the ISM. The Director, DIS (or when absent, the Acting Director) may approve waivers *to, or* deviations from, the provisions of this regulation or the ISM which do not require action by the DUSD or designee. All requests for waivers or deviations, including supporting justification, shall be submitted to the Director, DIS, ATTN: Deputy Director (Industrial Security) through the appropriate CSO.

b. Executive branch agency heads who are designated by the President of the U.S. as original TOP SECRET classification authorities pursuant to E.O. 12356 (reference (w)) may establish special access programs with special access, distribution, or protection requirements beyond those normally provided for access to TOP SECRET, SECRET, or CONFIDENTIAL information. Such officials or their designees shall make these programs applicable by incorporation in the contract or other appropriate notification and by providing copies of these to the CSO.

c. The Secretaries of the Military Departments and the Heads of DoD Agencies shall make the approved special access program requirements applicable by incorporating them in the contract and furnishing a copy of the requirements to the CSO.

d. To the extent required by the Director, DIS to execute his or her security responsibilities with respect to contracts, the UA shall provide for the granting of authorization for access to special access programs by DIS industrial security personnel.

e. Additional investigative requirements shall not be required by UA's for any project or program, other than those established herein, without the prior approval of the DUSD(P), his or her designee, or higher authority.

f. The use of "carve-out" contracts, which relieve the DIS from inspection responsibility under the Defense Industrial Security Program, is prohibited unless such contracts are in support of approved Special Access Programs.8/ In these instances, the User Agency shall provide a copy of DD Form 254, "Contract Security Classification Specification," to the appropriate cognizant security office and indicate in Item 15, what agency will have the inspection responsibility for the carve-out contract. Specific elements and areas which are "carved-out" shall also be specified.

1-115 Security Administration of U.S. Classified Contracts Awarded to U.S. Contractors for Performance Abroad. The security administration of a U.S. classified contract awarded to a U.S. contractor which will require performance outside of the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory will be accomplished as follows.

a. The Director of Industrial Security for the DIS Region in which the HOF or principal U.S. based office of the contractor is located shall assume security cognizance of the contractor. The functions to be performed by the CSO will encompass all the usual aspects of security cognizance established by this regulation as they pertain to the contractor's U.S. based facility. This will include the processing of the contractor for a, FCL; that is, the execution of the DD Form 441; the DD Form 441s; the resolution of all questions involving foreign ownership, control, or influence (FOCI), in accordance with this regulation;-and the processing of all OODEPs

---

8/ DoD Components must comply with Chapter XII, "Special Access Programs" of DoD 5200.1-R, "Information Security Regulation." Non-DoD User Agencies must comply with their Agency procedures and regulations.

for PCL's pursuant to this regulation. In this connection, the contractor's SPP which relates to the contractor's overseas operation will be routed through the UA to the CSO for review. (All aspects of security administration which must be performed outside of the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory, most notably the inspection function, will be the responsibility of the UA as discussed in paragraph c below, unless the UA requests this responsibility be assumed by DIS. The DIS will assume this responsibility upon receipt of such a request identifying specific U.S. installations. Requests for such support should be submitted to the Director, DIS, ATTN: Deputy Director (Industrial Security)).

b. The Director, DISCO shall be responsible for the industrial PCL function prescribed by this regulation regardless of where the contractor's employees are physically located. In this regard, all LOC's will be issued to the contractor's U.S. based cleared facility.

c. The UA awarding the contract shall be responsible for adapting, as may be necessary, the provisions" of this regulation and the ISM to its classified contracts performed by the contractor on a UA installation outside the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory. In the event a contractor is working on classified contracts of two or more UA'S at one location, or is performing on a classified contract awarded by one UA for performance on another UA installation, the UA's concerned and, if appropriate, DIS shall develop mutually acceptable arrangements for the "fulfillment of the responsibilities set forth in this paragraph. These responsibilities include all inspections of overseas sites where the contract is being performed. The basic security requirements imposed on the contractor are set forth in the ISM. In this connection, however, the UA is responsible for including in the contract, or other appropriate notification, any physical security requirements which are in addition to the ISM and which are necessary by virtue of the foreign location at which the classified contract is being performed. This would include specific requirements regarding the storage of classified information on government installations and the transmission of classified information through U.S. Government controlled channels. In such cases, the contracting UA shall furnish the additional security requirements to the CSO of the contractor's U.S. based facility, and the DIS activity responsible for inspections. In addition, the contracting UA shall include in the contract, or other appropriate notification, any special access program requirements established by the Secretary or Head of such UA (see paragraph 1-114), and furnish notice of the additional access requirements to. the CSO of the contractor's U.S. based facility and the DIS activity having inspection responsibility.

d. A contractor activity located outside of the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory shall not be granted a FCL in accordance with this regulation.

1-116 Privileged Information.

a. Reports submitted or information provided pursuant to the requirements of subparagraphs 5aa; 6a(l), (2), and (3); and 6b(1), of the ISM either classified if they so qualify, -or offered in confidence and so

marked by the contractors will be treated as privileged. When such reports are submitted in confidence, applicable exemptions of DoD 5400. 7-R (reference (1)) till be invoked as a matter of policy to withhold them from public disclosure. Such reports, other than those already classified, will be marked "FOR OFFICIAL USE ONLY, " following their receipt" and determination that they fall within one of the exemptions.

"b. When reports submit ted pursuant to the requirements of the ISM cited in paragraph a above contain unclassified information pertaining to an individual, it may not be withheld from that individual under the provisions of DoD 5400. ll-R (reference (m)), except that the identity of a source who furnished information to the government under an express promise of confidentiality may be protected by necessary deletions from that information. An implied promise of confidentiality given prior to September 27, 1975 is an adequate basis for deleting that information which identified its confidential source.

c. Should action for defamation of character be brought against a contractor or its employees for reporting information concerning an individual in accordance with the requirements of the ISM cited in paragraph a above, and the defendants in the suit seek the assistance of DoD in defending against the suits, their request should be referred to the Office of the Deputy Assistant Secretary of Defense (Security Policy) (ODASD(SP)), Office of the Assistance Secretary of Defense (Comptroller) (OASD(C)), for appropriate action.

Part 2. DEFINITION OF TERMS

1-200 Definitions. The definitions set forth below are established for the purpose of "this regulation.

1-201 Access, Accessibility. This refers to the ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures which are in force do not prevent him or her from gaining knowledge of the classified information 9/. *

1-202 Accountable COMSEC Material. COMSEC material received, sent, and controlled under the COMSEC Material Control System is considered accountable COMSEC material. Such material is normally identified by a short title assigned under the Telecommunication Security (TSEC) nomenclature system.

9/ The entry Into a controlled area, per se, will not constitute access to * classified information if the security measures which are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a PCL.

1-203 Alien. Any person not a citizen or national of the U.S. (see "Immigrant Alien," paragraph 1-237) is considered an alien.

1-204 Authorized Persons. Those persons who have a need-to-know for the classified information involved, and have been cleared for the receipt of such information (see paragraph 1-239) are authorized persons. Responsibility for determining whether a person's duties require that he or she possess, *or* have access to, any classified information, and whether he or she is authorized to receive it, rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipient.

1-205 Candidate Material. That material which is referred to collectively as special nuclear materials and nuclear weapons is candidate material.

1-205.1 Carve-Out. A classified *contract* issued in connection with an approved Special Access Program in which the DIS has been relieved of inspection responsibility in whole or in part. *

1-206 Central Office of Record (COR). The activity within a department or agency charged with the responsibility for maintaining records of accountability of all accountable COMSEC material received by or generated within the department or agency is the COR.

1-207 Channels for the Dissemination of COMSEC Material.

a. COMSEC Distribution and Accounting Channels. This refers to the distribution channels or shipping routes through which the COMSEC material is handled and shipped so that from the time of origin to eventual disposition the material is moved under a continuous receipt system from COMSEC custodian to COMSEC custodian. These channels are referred to as the COMSEC material control system.

b. Classified Information Channels. This refers to normal classified information channels through which classified COMSEC correspondence and matter other than accountable COMSEC material is transmitted.

1-208 Classified Contract. Any contract that requires or will require access to classified information by the contractor or his or her employees in the performance of the contract is a classified contract. (A contract may be a classified contract even though the contract document is not classified.)

1-208.1 Classification Guide. A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively is a classification guide.

1-209 Classified Information. This refers to information or material that is: (i) owned by, produced by or for, or under the control of the U.S. Government; (ii) determined under E.O. 12356 or prior orders to require protection against unauthorized disclosure; and (iii) so designated.

1-209.1 Classifier. "An individual who makes a classification determination and applies a security classification to information or material is a classifier." A classifier may be a classification authority or may derivatively assign a security classification based on a properly classified source or a classification guide. Within this context, contractors may apply security classification markings based on classified source material or a DD Form 254, as required by this regulation.

1-210 Closed Area. A closed area is a controlled area established to safeguard classified material which, because of its size or nature, cannot be adequately protected by the safeguards prescribed in paragraph 16, ISM, or be stored during nonworking hours in accordance with paragraph 14, ISM, (see section IV, ISM).

1-211 Cognizant Security Office (CSO). This refers to the office of the DIS Director of Industrial Security that has industrial security jurisdiction over the geographic area in which a facility is located.

1-212 Colleges and Universities. This refers to all educational institutions which award academic degrees, as well as related research activities directly associated with a college or university through organization or by articles of incorporation.

1-213 Reserved.

1-214 Communications Intelligence. This is technical and intelligence information derived from foreign communications by other than the intended recipients.

1-215 Communications Security (COMSEC). COMSEC refers to protective measures taken to deny unauthorized persons information derived front telecommunications related to national security and to ensure the authenticity of such communication. Such protection results from the application of security measures to electrical systems generating, handling, processing, or using national security information and also includes the application of physical security measures to COMSEC information or materials.

1-216 Communications Security (COMSEC) Information. COMSEC information is all information concerning COMSEC and all COMSEC material. (This includes classified information pertaining to COMSEC but not sent, received, or safeguarded within the COMSEC material control system. Examples are COMSEC installation standards, material, and classified design information produced under contract which will become CRYPTOSYSTEM/COMSEC materials upon acceptance by the U.S. Government.)

1-217 Compromise. Compromise is the disclosure of classified information to persons not authorized access thereto.

1-217.1 Compromising Emanations. This refers to unintentional or intelligence-bearing signals which, if intercepted or analyzed, disclose national security information transmitted, received, handled, or otherwise processed by any information processing system.

1-218 CONFIDENTIAL. "CONFIDENTIAL" Is the designation' that shall be applied to information or material the unauthorized disclosure of which reasonably could be expected t-o cause damage to the" national security.

1-219 Continental Limits of the United States. This refers to U.S. territory, including the adjacent territorial waters located within the North American continent between Canada and Mexico.

1-220 Contracting Officer. A contracting officer is any person who, in accordance with departmental or agency procedures, is currently designated a contracting officer, with the authority to enter into and administer contracts and make determinations and findings with respect thereto, or any part of such authority. The term also includes the authorized representative of the contracting officer acting within the limits of his or her authority. For purposes of this regulation and the ISM, the term contracting officer refers to the contracting officer at the purchasing office who is identified as the PCO and the contracting officer at a contract administration office who is identified as the ACO. Normally, the responsibilities which the regulation assigns to the contracting officer during the precontract, contract award, and postcontract stages of a classified procurement will be performed by the PCO, with the ACO performing those responsibilities which arise during the performance stages of a classified contract. Postcontract responsibilities include those industrial security actions which the purchasing office assumes when it authorizes a contractor to retain classified material after the termination or completion of a classified contract.

1-221 Contractor. A contractor is any industrial, educational, commercial, or other entity that has executed a "Department of Defense Security Agreement" (DD Form 441) with a DoD Agency for the purpose of performing on a classified contract or other classified procurement.

1-221.1 CNWDI. CNWDI is TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and totally contained quantities of fissionable, fusionable, and high-explosive materials by type. Among these excluded items are the components which DoD personnel, including contractor personnel, set, maintain, operate, or replace.

1-221.2 Critical Technology. Militarily-significant technology that is not possessed by potential adversaries and which, if acquired by them, would permit a substantial advance in their military capabilities, much to the detriment of the U.S. National Security. Critical technology satisfies one or more of the following criteria:

a. it contributes to the superior characteristics (performance, reliability, maintainability or cost) of current military systems;

b. it relates to specific military deficiencies of a potential adversary and would contribute significantly to the enhancement of their military mission;

c. It is an emerging. technology with high potential for having a major Impact upon advanced weapons systems.

(The Military Critical Technologies List **(MCTL) is** a reference document to be used in making this judgment).

1-222 **CRYPTO** . **CRYPTO** is a marking *or* designator identifying all **COMSEC** keying material used to protect or authenticate telecommunications carrying national security-related information. (The **CRYPTO** marking also identifies **COMSEC** equipment with installed hardwired operational keying variables.)

1-223 CRYPTOSYSTEM. This **refers** to the associated items of **COMSEC** equipment or material used as a unit to provide a single means of encryption or decryption.

1-223.1 Custodian. An individual who has possession of or **is otherwise** charged with the responsibility for safeguarding or accounting for classified information is the custodian.

1-224 Declassification. This is the determination that classified information no longer requires, **in** the interests of national "security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

1-225 Department of Defense. DoD refers **to** the Office of the Secretary of Defense (including all boards, councils, staffs, and commands), **DoD** agencies, and the Departments of the Army, Navy, and Air Force (including all of their activities) .

1-225.1 Derivative Class if **icat** ion. This is a determination that information is in substance the same as information currently classified and the **applica-** t ion of the **same** class if icat ion marking.

1-226 Document. A document is any recorded information, regardless of its physical form or characteristics, exclusive of machinery, apparatus, equipment, or other Items of material. The term includes, but is not limited to, the following: . all written **material,** whether handwritten, **printed,** or **typed; all** photographs, negatives, exposed or printed f **ilms,** and still or - motion pictures; all data processing cards or tapes; maps; charts; paintings; drawings; engraving; sketches ; working notes and papers; all reproduction of the foregoing by whatever process reproduced ; and **sound/voice** of electronic recordings in any form.

1-227 Downgrade. To downgrade is to determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a lower degree of protection.

1-227.1 Essential Elements of Friendly Information **(EEFI)** . Key questions, or critical inf **ormat ion/secrets** about United States intentions, military capabilities, plans or programs needed by an adversary **to relate** with other **available** information and intelligence in order to assist that

adversary in reaching a logical decision. DoD military components refer to the Essential Elements of Friendly Information as EEFI. These EEFI may be disclosed through OPSEC indicators. *

1-228 Executive Personnel. This refers to those individuals in managerial positions other than owners, off icers, or directors who administer the operations of the facility. (This category includes such designations as general manager, plant manager, plant superintendent, or similar designations, the FSO, and any individual who exercises control over the FSO.) *

1-229 Facility. A facility is a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, which, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined above). For purposes of industrial security, the term does not include UA installations.

1-230 Facility Security Clearance (FCL). This is an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

1-231 Foreign Government Information. This is information that is: (i) provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or (ii) produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments, requiring that the information, the arrangement, or both, are to be held in confidence.

1-231.1 Foreign Interest. The term refers to any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the U.S., or its possessions; or any form of business enterprise organized or incorporated under the laws of the U.S., or a state or other jurisdiction of. the U.S., which is owned or controlled by a foreign government, firm, corporation, or person. Included in this definition is any natural person who is not a citizen or national of the U.S. (An immigrant alien as defined in paragraph 1-237 is excluded from the definition of a foreign interest.)

1-232 Foreign Nationals. All persons not citizens of, not nationals of, nor immigrant aliens to the U.S. are foreign nationals.

1-233 FORMERLY RESTRICTED DATA. This is information removed from the RESTRICTED DATA category upon joint determination by DOE (or antecedent agencies) and DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such Information is treated in the same manner as RESTRICTED DATA.

1-234 Graphic Arts. This refers to facilities and individuals engaged in performing consultation, service, or the production of any component or end product which contributes or results in, the reproduction of classified information. Regardless of trade names or specialized processes, it includes writing, illustrating, advertising service, copy preparation, all methods of printing, finishing services, duplicating, photocopying, and film processing activities.

1-235 Handling. Handling refers to the preparation, processing, transmission, and custody of classified information.

1-236 Home Office (HOF). The headquarters facility of a MFO (see paragraph 1-246) is the HOF.

1-237 Immigrant Alien. Any person lawfully admitted into the U.S. under an immigration visa for permanent residence is an immigrant alien (see paragraph 2-308 for special prerequisites for clearance of immigrant aliens).

1-238 Industrial Security. That portion of internal security which is concerned with the protection of classified information in the hands of U.S. industry is industrial security.

1-239 Information Security. This refers to the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order or statute.

1-240 Intelligence. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of foreign operations and which is immediately or potentially significant to military planning and operations.

1-241 Interim Security Clearance. This is a security clearance based on lesser investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

1-242 Internal Security. This refers to the prevention of action against U.S. resources, industries, and institutions and the protection of life and property in the event of a domestic emergency by the employment of all measures, in peace or war, other than military defense.

1-243 Locked Entrance. A locked entrance is an entrance to a Closed or Restricted Area which is kept closed and locked at all times except when temporarily unlocked and opened under supervision for the purpose of passing material or authorized personnel into or out of the area.

1-244 Long Title. The full title or name assigned to a publication, an item of equipment, or device is the long title.

1-245 Material. Material refers to a product or substance on, or in which, information is embodied.

1-246 Multiple Facility Organization (MFO). A legal entity (single proprietorship, partnership, association, trust, or corporation) which is composed of two more facilities (see paragraph 1-229) is a MFO.

1-247 National of the United States. A national of the U.S. is:

a. a citizen of the U.S.; or

b. a person who, although not a citizen of the U.S., owes permanent allegiance to the U.S. 10/.

1-248 NATO Classified Information. The term "NATO classified information," embraces all classified information, military, political, and economic that is circulated within and by NATO whether such information originates in the organization itself or is received from members nations or from other international organizations.

1-249 Need-to-Know. This is a determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to (see paragraph 1-201), knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a UA.

1-250 Negotiator. Any employee, in addition to the 00DEPs, who requires access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime or subcontract is a negotiator. (This category may include, but is not limited to, accountants, stenographers, clerks, engineers, draftsmen, and production personnel.)

1-251 Officers (Corporation, Association, or Other Types of Business or Educational Institution). This definition includes persons in positions established as officers in the articles of incorporation or bylaws of the organization, including all principal officers; that is, those persons occupying positions normally identified as president, senior vice president, secretary, treasurer, and those persons occupying similar positions. In unusual cases, the determination of principal officer status may require a careful analysis of an individual's assigned duties, responsibilities, and authority as officially recorded by the organization.

1-252 Official Information. Information which is owned by, produced for or by, or is subject to the control of the U.S. Government is official information.

10/ See 8 U.S.C. (Section 1101(a)(22)), reference (n). 8 U.S.C. § 1401, subsection (a) lists in paragraphs (1) through (7) categories of persons born in and outside the U.S. or its possessions who may qualify as nationals of the U.S. Where doubt exists as to whether or not a person can qualify as a national of the U.S., this subsection should be consulted.

1-252a. Operations Security (OPSEC). The- process of denying adversaries * information about f riendly capabilities and intentions by identifying, * controlling, and protecting indicators associated with planning and con- * ducting military operations and other activities. Section X of this * regulation contains a detailed discussion of OPSEC and UA responsibilities * pertaining thereto. See JCS Pub 18 for further terms and definitions related to OPSEC.

1-252b. OPSEC Indicators. Actions or information (classified or * unclassified) obtainable by an adversary, that would allow the adversary * to develop or confirm assumptions, estimates and facts about United States * intentions, military capabilities, plans, or programs, thereby compromising * essential secrecy. *

1-252.1 Parent. A parent firm is a corporation which can control another corporation (subsidiary) by ownership of a majority of its stock. The control may exist by direct stock ownership of an immediate subsidiary or by indirect ownership through one or more intermediate levels of subsidiaries.

1-253 Possessions. Possessions include the Virgin Islands, Guam, American Samoa, and the Guano Islands with Swains Island, Howland Island, Baker Island, Jarvis Island, Midway Islands, Kingman Reef, Johnston Island, Sand Island, Navassa Island, Swan Islands, and Wake Island.

1-253.1 Principal Management Facility (PMF). The PMF is a cleared facility of a MFO which reports directly to the HOF, and whose principal management official has been delegated the responsibility to administer the contractor's industrial security program, within a defined geographical or functional area.

1-254 Reference Material. This refers to documentary material over which the UA does not have classification jurisdiction and did not have classification jurisdiction at the time such material was originated. Much material made available to the contractors by the DTIC and other secondary distribution agencies is reference material as thus defined.

1-255 Regrade. To regrade is to assign a higher or lower security classification to an item of classified material.

1-256 Representatives of a Foreign Interest (RFI). This refers to citizens or nationals of the U.S. or immigrant aliens who, in their individual capacity, or on behalf of a corporation (whether as a corporate officer or official or as a corporate employee who is personally involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporations or person. However, a U.S. citizen or national who has been appointed by his or her U.S. employer to be a representative in the management of a foreign subsidiary (for example, a foreign firm in which the U.S. firm has ownership of at least 51% of the voting stock) will not be considered a RFI, solely because of this employment, provided the appointing employer is his or her principal employer and is a firm that possesses or is in process for a FCL.

1-257 Restricted Area. This is a controlled area established to safeguard classified material which, because of its size or nature, cannot be adequately protected during working hours by the safeguards prescribed in paragraph 16, ISM, but which is capable of being stored during non-working hours in accordance with paragraph 14, ISM (see section IV, ISM).

1-258 RESTRICTED DATA. All data (information) concerning: (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but not to include data declassified or removed from the RESTRICTED DATA category pursuant to Section 142 of the Atomic Energy Act (see Sally, Atomic Energy Act of 1954, reference (o), and paragraph 1-233, ISR, on FORMERLY RESTRICTED DATA).

1-259 SECRET. "SECRET" is the designation that shall be applied only to information or material, which the unauthorized disclosure of could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

1-260 Security. Security refers to the safeguarding of information classified TOP SECRET, SECRET, or. CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.

1-261 Security Cognizance. This is the responsibility for acting for UA's in the discharge of industrial security responsibilities described in this regulation.

1-261.1 SENSITIVE COMPARTMENTED INFORMATION. This term includes all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include RESTRICTED DATA as defined in Section 22, Public Law 83-703, Atomic Energy Act of 19S4, reference (o).

1-262 " " Short Title. This is an identifying combination of letters and numbers assigned toe publication or equipment for purposes of brevity.

1-263 Special Access Program. This refers to any program imposing need-to-know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; material dissemination restrictions; or special lists of persons determined to have a "need-to-know."

1-264 Subsidiary. A subsidiary is a corporation which is controlled by another corporation (parent) by reason of the latter corporation's ownership of at least a majority (over 50%) of the capital stock. A subsidiary is a legal entity and shall be processed separately for a FCL.

1-265 Telecommunications. The transmission, communication, or processing of information, including the preparation of such information thereof, by electrical, electromagnetic, electromechanical, or electro-optical means.

1-265.1 TEMPEST . TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations (see paragraph 1-217.1).

1-266 Time Resource Sharing. For the purpose of this regulation, the term applies to the concurrent use of an ADP system by one or more users. The term includes the functional characteristics of an ADP system which allow simultaneous or apparently simultaneous access to all or part of the ADP system by more than one user or the acceptance and processing of more than one computer program of instructions. The term encompasses the characteristics of time-sharing, multiprocessing, multiprogramming, or combinations of these functional capabilities in any form.

1-267 TOP SECRET. "TOP SECRET" is the designation that shall be applied only to information or material, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the U.S. or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital material defense plans or complex cryptologic and communications intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific and technological developments vital to national security. .

1-268 Transmission Security. Transmission security is that component of security which result from all measures designed to protect communication transmissions from interception and traffic analysis.

1-269 Trust Territory. This definition applies only to the trust territory of the Pacific Islands which the U.S. administers under the terms of a trusteeship agreement concluded between this government and the Security Council of the- United Nations pursuant to authority granted by Joint Resolution of Congress, July 18, 1947 (61 Statute. 397, Title 48 U.S.C., § 1681) (reference (p)). According to this agreement, the U.S. has "full power of administration, legislation, and jurisdiction" over the territory; this government, however, does not claim "sovereignty ." Three major archipelagoes make up the

trust territory: Carolines (including the Palau Islands), Marshalls, and Marianas (excluding Guam).

1-270 Unauthorized Person. Any person not authorized to have access to specific classified information in accordance with the provisions of the ISM and this regulation is an unauthorized person.

1-271 United States. This is the 50 states and District of Columbia.

1-272 Upgrade. upgrade is to determine that certain classified information requires, in e intereats of national security, a higher degree of protection against u uthorized disclosure than currently provided, coupled with a changing of t classification designation to reflect such a higher degree.

1-273 User Agents (UA's). This term refera to the OSD (including all boards, councils, staffs, and commands), DoD agencies, and Departments of Army, Navy, and Air rce (including all of their activities); National Aeronautics and Spat Administration; General Services Administration; Small Business Admin tration; National Science Foundation; Environmental Protection Agency; a the Departments of State, Commerce, Treasury, Transportation, Inte or, Agriculture, Labor, and Justice; U.S. Arms Control and Disarman t Agency, Federal Emergency Management Agency, the * Federal Reserve Syst ; General Accounting Office; and the U.S. Information * Agency. *

Part 3. SECURITY COGNIZANCE

1-300 Policy.

a. Admini ration of the DoD Industrial Security Program is assigned to the Director, DIS Security cognizance authority is delegated to the Regional Directors c Industrial Security for all contractor facilities physically located w hin the geographic boundaries of their respective jurisdictions (see a endix B). The Regional Director of Industrial Security shall perform all co izant security functions prescribed in this regulation and the ISM on behal of all UA's unless the provisions of paragraphs 1-108 or 1-115 apply, In whit case the Commander or Head of the UA installation shall perform certain secu ty actions.

b. All re tionships between the UA and the contractor on industrial security matters sha be handled through or in coordination with the CSO except those matters specif ally set forth in this regulation and the ISM as responsibilities of the UA ontracting activity.

c. The as nption of industrial security cognizance by the Director of Industrial Securi will not relieve any UA of the responsibility for protecting and safeg rding its classified material incident to its classified contracts with-the f ility, or from visiting the facility to review the -security aspects of ch contracts. However, visits by a representative of a UA to a facility to view security aspects of a contract shall be coordinated , with the CSO prior t such visits. Any deviation from the requirements of the ISM or special secur y requirements under the contract, which may be noted

during the visit shall be referred promptly to the CSO, with suggested corrective action or additional security requirements to be" levied on the contractor. The CSO shall take appropriate action regarding these matters, and, If requested, shall notify the UA of the corrective action taken by the contractor.

d. International operations are the responsibility of the Deputy Director (Industrial Security), HQ DIS.

e. PCL actions are the responsibility of the Director, DISCO.

f. With respect to commercial carriers, the authority for security cognizance has been delegated to" each CSO for those elements of carriers physically located within the geographic boundaries of each region. All relationships between the government and commercial carriers on safeguarding SECRET controlled shipments shall be handled through or In coordination with the CSO. Commercial carriers which have been assigned to one of the CSO's for security cognizance shall be notified in writing of this action.

g. With the exception of candidate material (CM) (CONFIDENTIAL or SECRET category), when an escort is used, the company furnishing the transportation service (ship, rail, air, or truck) is not required to have a FCL. An escort shall always be used when ship or rail transportation is involved. Consequently, ship and railroad companies will not be issued a FCL. When a shipment by truck is contemplated for classified CM (CONFIDENTIAL or SECRET), the contracting officer will issue specific shipping instructions, requiring a driver holding a final SECRET clearance in addition to the military escort normally provided for such shipments. .

h. The CSO of the HOF of a carrier is responsible for maintaining a central master file containing copies of pertinent reports and correspondence concerning all violations, major deficiencies, unsatisfactory conditions, and major problem areas in the carrier's system, regardless of the geographical area of the terminal involved. It 1s the responsibility of the CSO of the terminals to assure that copies of such pertinent reports and correspondence are furnished the CSO of the HOF.

1-301 Functions of a Cognizant Security Office. Procedures set forth in this regulation prescribe the functions and responsibilities of the CSO.

1-302 Notification of Security Assignment. The management of each facility which has been assigned to a CSO for security cognizance shall be notified in . writing of this assignment when a FCL action is to be initiated for the facility.

1-303 Procedural Changes. All questions of interpretation with respect to procedures or methods prescribed in the ISM or this regulation shall be answered by the CSO, except that interpretations of security classification guidance, procedures, or methods shall be provided by the contracting officer of the UA, or his or her designated representative. For facilities or contractor activities located on a UA Installation (see paragraphs 1-108 and 1-115), requests from the contractor for interpretations of the requirements of the ISM shall be forwarded to the CSO through the Commander or Head of the installation. In all instances where this regulation or the ISM requires that

management of a facility be advised regarding changed industrial security procedures or methods, the CSO shall so advise management.

1-304 Defensive Security Briefing.

a. When a report is received from a contractor, the CSO, or UA, in accordance with paragraph 6b(9), ISM, that a cleared employee or Type A Consultant has traveled to or through a Designated 11/ country, or attended * an international scientific, technical, engineering, or other professional meeting when a representative of a Designated country participated or was in attendance (hereinafter called foreign travel), the DISCO shall review the records available in the PSCF, in light of the employee's travel. If the PSCF records indicate a background investigation (BI) or expanded national agency check (ENAC) or any investigative coverage other than a satisfactory national agency check (NAC), the investigative file shall be obtained and reviewed. If the PSCF records indicate that the only investigation conducted in the case is a satisfactory NAC, it will not be necessary to obtain the investigative file. However, where possible, the "Department of Defense Personnel Security Questionnaire (Industrial-NAC)" (DD Form 48) or "Department of Defense Personnel Security Questionnaire (Industrial)" (DD Form 49) submitted by the individual in connection with the application for clearance shall be reviewed.

(1) The DISCO shall request additional investigation in those cases in which the employee's report of intended foreign travel discloses discrepancies between this report and information previously furnished or developed by the government. For example, where the "Department of Defense Personnel Security Questionnaire (Industrial-NAC)" or "Department of Defense Personnel Security Questionnaire (Industrial)" submitted In connection with the clearance application indicates the individual has no relatives residing in Designated countries, and yet the purpose of the intended foreign travel is to visit a relative in a Communist country, it is necessary to determine through investigation whether the original clearance application was fraudulent and if the case currently presents a hostage problem as discussed In paragraph 2-305. Moreover, in those cases where the Investigation conducted in connection with the clearance application raised serious questions concerning such things as the individual's suitability, trustworthiness, or national allegiance, it may be necessary to update the investigation and reevaluate the case in light of this new element of foreign travel which brings the individual in direct contact with or to the attention of officials or representatives of a Designated country.

11/ Designated countries (those countries whose policies are inimical to * U.S. interests) are: Iran, Afghanistan, Angola, Ethiopia, Iraq, Nicaragua, South Yemen, Syria, Libya, Albania, Bulgaria, Kampuchea (formerly Cambodia), People's Republic of China (including Tibet), * Cuba, Czechoslovakia, North Korea, German Democratic Republic (GDR) (East Germany, including the Soviet Sector of Berlin), Hungary, Laos, Mongolian People's Republic (Outer Mongolia), Poland, Rumania, Union of Soviet Socialist Republics (USSR.) (including Estonia, Latvia, Lithuania, and all the other constituent republics, Kurile Islands and South Sakhalin (Karafuto)), Vietnam, and Yugoslavia.

(2) The report of the employee's foreign travel furnished by the contractor pursuant to paragraph 6b(9), ISM, shall be recorded in the PSCF . While most cases do not fall within the purview of paragraph a above, and do not require additional investigation, it may be necessary because of the number or frequency of such visits to initiate additional investigation to determine if there is any security significance to the foreign travel in light of the individual's current PCL status.

(3) Where results of the additional investigation initiated pursuant to paragraphs 1 or 2 above indicate that the Individual's continued access to classified information is not clearly consistent with the national interest, action shall be initiated in accordance with paragraph 2-320.

b. When a report is received from the contractor in accordance with paragraph 6a(19), ISM, that a Designated country representative(s) or national(s) will visit the facility, the CSO shall immediately follow up with the contractor by telephone or visit as appropriate to ensure that adequate safeguards have been established for controlling such visitors, especially when the visit is to be over an extended period of time. The contractor shall also be reminded to strictly apply the guidance in appendix VII, 15X, and to obtain the contractor's assistance in identifying any security problems involved, in such visits. Further, during the course of the next recurring inspection the contractor's procedures for conducting the briefings required by appendix VII, ISM, shall be reviewed and verification made that the briefings required by paragraph 5u, ISM, were accomplished.

1-305 Responsibility for the Security of SENSITIVE COMPARTMENTED INFORMATION Contracts.

a. Where a procurement activity awards a SENSITIVE COMPARTMENTED INFORMATION contract for the National Security Agency (NSA), exclusive security responsibility remains with NSA and that agency shall prescribe the security requirements for the contract. The NSA will process access authorizations for SENSITIVE COMPARTMENTED INFORMATION for contractor employees used on such contracts. The CSO and contracting activity are relieved of security responsibilities pertaining to such SENSITIVE COMPARTMENTED INFORMATION contracts.

b. Where a SENSITIVE COMPARTMENTED INFORMATION contract is awarded by and for a UA other than NSA, the UA will designate an activity which shall have exclusive security responsibility for, and shall prescribe the security requirements for the contract. The designated activity will process access authorizations for SENSITIVE COMPARTMENTED INFORMATION for contractor employees used on such contracts. The CSO and the contracting officer, except as may be specifically delegated by the designated activity, are relieved of security responsibilities pertaining to such SENSITIVE COMPARTMENTED INFORMATION contract.

c. When a SENSITIVE COMPARTMENTED INFORMATION contract is awarded, item 15 of the "DoD Contract Security Classification Specification" (DD Form

254), shall specify the activity which has **exclusive security** responsibility for this contract.

d. Access authorizations for SENSITIVE COMPARTMENTED INFORMATION will be processed in the following manner.

(1) The contracting office shall instruct the contractor to submit clearance applications to the appropriate activity of NSA or the UA activity other than NSA.

(2) The NSA, or where appropriate, the UA activity with security responsibility will provide the contractor appropriate notification of the access authorization for SENSITIVE COMPARTMENTED INFORMATION.

1-306 Operational Responsibility for NSA **COMSEC** Account. Where a procurement activity awards a **COMSEC** contract for the NSA and a **COMSEC** account is required, exclusive operational responsibility for the account remains with NSA. The NSA COR **will** establish the account **in** accordance with paragraph 1-504. The NSA COR or its designated representative shall ensure that the custodians are instructed on all operational aspects regarding control, accountability, and handling of accountable COMSEC material. Tt will conduct audits **annually,** or more frequently when required, **to ensure** custodians are following prescribed “procedures in the operations of the **COMSEC** account. The procurement activity Is relieved of operational responsibility pertaining to the **COMSEC** account. The **CSO will** be guided by DoD 5220.22-S-1 (reference (q)) and by instructions furnished to the contractor by NSA COR, prescribing the type **of COMSEC** material, records, reports, and procedures to-be utilized by the custodian in maintaining control and accountability of the **COMSEC** material.

Part 4. SPONSORSHIP OF MEETINGS

1-400 Application. The following provisions apply *to* a conference, **seminar, symposium, exhibit,** or **convention** at which classified information is disclosed and which is conducted by a DoD Component, a cleared DoD contractor, or by an association, institute, or society whose membership consists of DoD contractors, contractor employees, or DoD personnel. These provisions do not apply to meetings related to a specific contract or project, including **preproposal** or **preaward** meetings, and postaward briefings conducted by the DoD contracting activity. Also, meetings conducted by a cleared contractor(s) and attended by cleared contractor personnel directly involved in the performance **of** a contract or project are excluded from the provisions of this part. Provisions of paragraph 1-408 apply to meetings described in paragraph 5q(3) and (4), ISM. Sponsorship of meetings by a UA other than DoD **will** be in accordance with the procedures of that agency.

1-401 General Policy. All meetings conducted within the scope of this part must be sponsored for security by **a** DoD Component. The Head of a DoD Component, or designee, having a significant interest in the subject matter, may sponsor a meeting for security after determining that:

a. the conduct of classified sessions of the meeting is in the best interests of the national security,

b. the use of conventional channels for dissemination of classified scientific and technical information would not accomplish the purpose of the meeting,

c. adequate security measures and access procedures have been developed and will be carried out, and

d. the location selected for the classified sessions of the meeting facilitates the proper control and dissemination of classified information and adequate facilities are available for its storage and protection.

1-402 Requests for Sponsorship. When requested by an association, institute, or society whose membership is comprised primarily of contractors cleared by DoD, contractor employees, or DoD personnel, a DoD Component may sponsor s meeting for security purpose, provided the DoD Component or a designated cleared contractor undertakes overall security responsibility and security administration.

1-403 Guides for Sponsorship. Sponsorship for security purposes shall be by a single government activity having a principal interest in the subject matter. Acceptance of sponsorship for security purposes by the department or agency does not relieve any other activity from responsibility for authorizing or prohibiting the release or dissemination of information under its jurisdiction. When appropriate, the department or agency sponsoring the meeting for security purposes may request other DoD activities to provide such assistance, facilities, or support as may be justified in the interest of economy, efficiency, and security. Sponsorship for security purposes shall be granted only for a meeting conducted by a cleared contractor. However, a meeting conducted by an association, institute, or society whose membership consists of cleared contractors may be sponsored for security purposes, provided a cleared contractor is designated and accepts responsibility on behalf of the association, institute, or society for ensuring the security measures and procedures at the meeting.

a. Sponsorship normally shall be granted only for a meeting conducted by a cleared contractor. However, a meeting conducted by an association, society, or group whose membership consists primarily of cleared contractors may be sponsored provided a cleared contractor is designated and accepts responsibility on behalf of the association, society, or group for providing the security measures and procedures at the meeting.

b. Meetings shall be sponsored only when there is assurance that adequate security measures have been planned and will be conscientiously executed. Prior to accepting sponsorship, a determination shall be made that

the location selected for the meeting site ensures adequate safeguarding and control of dissemination of classified information 12/. *

1-404 Location of Meetings. The activity sponsoring the meeting for security is responsible for evaluating and approving the location proposed for the meeting.

a. A meeting at which TOP SECRET or SECRET information is to be disclosed shall be held only at a U.S. Government or cleared contractor facility; that is, a facility in a fixed location where adequate measures for safeguarding classified information can be imposed. Under this criteria, the proposed meeting site would have to be on a government installation or at a cleared contractor facility. In either case the meeting must be held in an area of the government installation or contractor facility that can be secured. An auditorium, assembly hall, or gymnasium which is used primarily for campus activities and public gatherings cannot be secured and shall not be approved for a classified meeting at which TOP SECRET or SECRET information would be disclosed, even though it is located on the campus of a university or college, portions of which are a cleared facility.

b. A meeting at which information classified no higher than CONFIDENTIAL is to be disclosed normally shall be held at a U.S. Government installation or at a cleared contractor facility. However, the Head of the DoD Component sponsoring the meeting for security may approve the use of another location for such a meeting, provided suitable facilities are not available at a government installation or cleared contractor facility, and the sponsoring activity determines that adequate security can be maintained at the proposed location. The authority to approve a location other than a U.S. Government installation or cleared contractor facility may not be delegated, except that a Secretary of a Military Department may delegate his or her authority to an Assistant Secretary of that Department. A contractor's request to use a location other-than a cleared contractor's facility or a U.S. Government installation shall be in compliance with paragraph 9c(2), ISM.

1-405 Security Procedures. The sponsoring activity is responsible for reviewing and approving the security measures and procedures developed by the contractor, for ensuring the security of the classified information, and for supervising and assisting in the development and application of those procedures. The security measures shall include adequate arrangements for the following.

a. Strictly limiting attendance at a classified meeting *to* authorized persons -- this shall include measures for determining that all persons on the approved list of attendees have been granted a security clearance equal to or higher than the category of information to be discussed, and have duties-requiring such access. For contractor personnel, the certification of security clearance and need-to-know shall be accomplished as provided in paragraph 1-409.

12/ Sponsorship of meetings by a UA other than the DoD will be in accordance with the procedures of that agency. * .

b. Reviewing and approving all announcements and invit at ions related to the meeting and lists of attendees pertaining thereto — announcements and invitations shall be unclassif led and shall include the specific name of the sponsoring activity and the date of approval.

(1) Notices and announcements of meetings, whether classified, unclassified, or mixed, and not amounting to invitations to attend, may be published publicly, provided classified information is not included in such notices or announcements.

(2) In the case of a classified meeting, invitations to attend, whether on an individual or class basis, shall not be sent to a person known to be a national from, or a representative of, a Communist country.

c. Safeguarding and controlling the distribution of notes, minutes, summaries, recordings, proceedings, and reports on the classified portions of the meeting -- such material normally shall be sent only to those approved for *attendance* at the classified sessions. However, the sponsoring activity may also authorize distribution to others who are determined to be eligible for and who require access to the classified information involved. In any event, the material shall be sent only to a government activity or cleared contractor facility and marked for the attention of the intended recipient, as provided in paragraph 17, ISM.

d. Security measures shall include notifying each person who presents or discloses classified information at the meeting of the security limitations on disclosures for such reasons as the level of clearance or need-to-know of members of the audience, or other limitations *required* by the National Disclosure Policy of the government or directives of UA's.

e. Ensuring the physical security of the meeting site and the area used for classified sessions or displays -- this shall include provisions for guards, entrance controls, personnel identification, storage facilities, and adequate security against unauthorized access to, or illicit acquisition of, the classified information. Classified sessions of mixed meetings, that is, those having both classified and unclassified sessions, shall be held at places geographically separated from the place where unclassified sessions are held.

f. Security measures shall include ensuring that attendance at a meeting or session at which classified information is to be disclosed is limited *to* persons whose names appear on the access list approved by the sponsor, and who present proper identification.

g. Security measures shall include ensuring that individuals making oral presentations at meetings provide classification guidance sufficient to enable attendees to identify what information is classified or unclassified, and if classified, at what category or categories of classification.

h. Security measures shall also include reviewing the minutes, summaries, recording, proceedings, and reports of the meeting to eliminate any classified information or to limit distribution in accordance with paragraph c above.

1-406 Controlling Disclosures. The sponsoring activity shall require a contractor desiring to disclose classified information to furnish written approval from the contracting officer concerned prior to the meeting. The sponsoring activity shall:

a. maintain a central record of disclosure authorizations granted for contractor's presentations and displays,

b. require the contractor to furnish a copy of each classified presentation as actually made at the meeting, and

c* monitor the meeting to assure that-classified information is disclosed only to the extent authorized.

1-407 Attendance by Foreign Nationals and Representatives of a Foreign Interest 13/.

a. As a general rule, a DoD Component will not agree to sponsor a meeting for security if foreign nationals or representatives of foreign governments are to be in attendance at sessions of such meetings which involve the disclosure of classified military information. As an exception *to* this general rule representatives of, and nationals from, foreign countries, other than Designated countries, may attend classified sessions only when the Head of a DoD Component sponsoring the meeting for security, or a designee, determines that such attendance is consistent with National Disclosure Policy (NDP-1) (reference (r)) and specifically authorizes it in writing.

b. Representatives of, and nationals from, other than Designated countries may attend unclassified sessions without specific authorizations provided the disclosure of unclassified technical data, which is governed by the Export Administration Act of 1969 (reference (s)), as amended, as administered by the Secretary of Commerce, and Section 38 of the Arms Export Control Act (reference (t)) as administered by the Secretary of State through the ITAR (reference (i)), are complied with.

c. Representatives of, and nationals from, Designated countries may not attend a classified session under any circumstances. However, they may attend unclassified sessions when the Head of the DoD Component security sponsoring the meeting approves individually and in writing, on a name basis, such attendance when clearly justified as being in the national interest. This authority may not be delegated. When the attendance of such individuals at an unclassified session or presentation of a meeting is requested by the contractor, the activity sponsoring for security will forward the request through channels, recommending approval or disapproval. Such requests shall comply with paragraph 9b of the ISM, and will show how approval will further reci-

13/ A person granted a reciprocal clearance or a RFI cleared for access to classified information under the DoD Industrial Security Program is not subject to the limitations of paragraph 1-407, provided the information is releasable under National Disclosure Policy. However, persons granted reciprocal clearances are subject to the access limitations prescribed in . . paragraphs 2-322 and 2-324.

procity for attendance of U.S. personnel at similar meetings within Designated countries. No invitation shall be tendered, either formally or Informally, by or on behalf of the contractor, to a foreign national or representative of a Designated country or to his o-r her government or firm until his or her attendance has been approved.

d. The DoD Component which approves a request for attendance by a national from, or representative of, a Designated country at unclassified sessions of a meeting shall provide the Soviet and Eastern European Exchange Staff, Department of State, New State Building, Washington, D.C. 20520, the names of the proposed invitees, date of attendance, the location of the meeting, the subject matter to be discussed, and titles of scientific, technical, or other papers to be presented. The admissibility to the U.S. of these proposed invitees must be determined prior to the issuance of the actual invitation, if they have not already been admitted with a visa.

e. The sponsoring activity shall:

(1) advise the contractor of the approval or disapproval of the attendance of foreign nationals or RFI's at the meeting;

(2) ensure 'that foreign nationals or representatives of a foreign interest other than Designated countries are excluded from all classified sessions, presentations, and displays except those which they have specifically been authorized to attend; and

(3) ensure that foreign nationals or representatives of Designated countries are excluded without exception from all classified sessions, presentations, and displays and from all unclassified portions of sponsored meetings, except those which they have specifically been authorized to attend.

1-408 Disclosure Authorizations. The release of classified information by government representatives participating in contractor-conducted meetings shall be authorized in accordance with pertinent directives of their individual departments or agencies. Contracting officer approval of proposed. disclosures by contractors of classified information at contractor-conducted or government-conducted meetings shall be accomplished as follows.

a. Proposals from a contractor to disclose classified information at a meeting conducted under paragraphs 5q(3) or (4), ISM, shall be processed in accordance with the pertinent directives of the contracting activity having jurisdiction over the information involved.

b. If the proposed disclosure is approved, the contractor shall be notified in order that he or she, in turn, may advise the sponsoring activity.

1-409 Approval for Attendance at Classified Meetings. When a contracting officer or an official monitoring a UA program receives an application from a contractor for one or more of his or her employees to attend a classified meeting, he or she is required to determine the contractor's FCL, and need-to-know. The determination by the contracting officer or monitoring official of the FCL may be based on knowledge acquired through a current classified contractual relationship, program participation, or by verifying the FCL with

the PIC-CVA. The need-to-know determination can be made after reviewing the justification submitted by the contractor with the application. The general criterion for this determination will be whether, in the interest of national security, the contractor requires access to the classified information to be disclosed at the meeting in order to perform tasks or services essential to the fulfillment of a classified contract or program. After the FCL has been determined, the contractor's certification as to the PCL status and need-to-know of the employees who will attend the meeting shall be accepted. The contracting officer or monitoring official, after completing his or her required actions, provided that the contractor has certified that the employee is cleared at the appropriate level and has the need-to-know, will forward the contractor's application and certification to the sponsoring activity, indicating that the FCL has been verified and the need-to-know has been determined.

1-410 Notification. DoD Components sponsoring meetings for security shall notify the DUSD(P) ATTN: Director for Security Plans and Programs (DSP&P), of each meeting's subject matter or title, location, and date. This notification should be given at the time the DoD Component agrees to sponsor for security and can be accomplished by providing a copy of the letter reflecting this agreement. When reports of loss or compromise of classified information as a result of such a meeting are prepared in accordance with section V of this regulation, the DUSD(P) ATTN: DSP&P, shall be notified by copies of such reports.

Part 5. PROCEDURES PERTAINING TO COMSEC INFORMATION

1-500 Application. The procedures in this regulation pertaining to COMSEC information shall apply to, and shall govern, the industrial security relationship between UA's and contractors under one or a combination of the following conditions:

a. when the contractor requires the use of CRYPTOSYSTEMS in the performance of his or her contract;

b. when the contractor is required to install, maintain, or operate CRYPTO equipment for the U.S. Government; or

c* when the contractor is required to accomplish research, development, or production of CRYPTOSYSTEMS, CRYPTO equipment, or related COMSEC material.

1-501 Instructions Concerning COMSEC Material.

a. Requirements for the safeguarding of COMSEC material in the hands of industry are established in reference (q).

b. Distribution of reference (q) will be made by the CSO's and shall be limited to UA's and contractors meeting the conditions-established in paragraph 1-500.

1-502 Release of COMSEC Information and Material to "U.S. Contractors. Basic policy and procedures pertaining to the release of COMSEC information and material to U.S. *contractors* and to the *use* of COMSEC *material by* U.S. contractors are set forth in detail in National Communications Security " Committee publication NCSC-2, "National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernmental Sources," reference (u). Additional guidance is contained in appropriate DoD and UA instructions. Any request for a waiver from the provisions of references (q) or (u) shall be submitted to the Director, DIS, ATTN : Deputy Director (Industrial Security).

a. Use of COMSEC Material by Contractors.

(1) Contractors engaged in work on classified contracts may be authorized and should be encouraged to use certain CRYPTOSYSTEMS for the encryption of classified or unclassified, national security-related information. Use of a CRYPTOSYSTEM may be authorized for the encryption of classified or unclassified, national security-related communications between contractors and the U.S. Government, between contractors, between' various facilities of a contractor, and between contractors and subcontractors. A CRYPTOSYSTEM when approved, may be used by the contractor for the transmission of information classified *no* higher than that approved for the CRYPTOSYSTEM. Use is not limited to the contract for which originally approved.

(2) The contractor shall-submit a request for approval of the use of a CRYPTOSYSTEM to the contracting officer concerned. In turn, the. request shall reprocessed in accordance with appropriate contracting activity instructions.

(3) When use of a CRYPTOSYSTEM is authorized, the contracting activity shall:

(a) specify the levels of classified information which may be encrypted; and

(b) ensure, prior to issuance of the CRYPTOSYSTEM, that:

1 procedures are established to provide for the physical safeguarding of COMSEC materials and for the secure and efficient operation of the CRYPTOSYSTEM; and

2 security clearances for the highest classification of information or material have been granted by the U.S. Government to all persons who may require access and that these persons have been given a COMSEC briefing.

b. Utilization of Contractor Personnel in Government COMSEC Operations. From the standpoint of security and control of operations during both normal and emergency conditions, the installation, maintenance, and operation of U.S. Government secure telecommunications systems normally should be performed by appropriately cleared U.S. citizens who are military personnel or civilian employees of the government.

(1) In those cases where the installation, maintenance, and operation of secure telecommunications systems by contractor personnel is considered in the best interest of the government, Heads of UA's may authorize the utilization of U.S. contractor personnel to perform these functions. The National Communications Security Committee (formerly USCSB) shall be advised of each instance where contractor personnel are utilized and of their terminations of such employment.

(2) When the utilization of contractor personnel in government COMSEC operations has been authorized, the contracting UA shall ensure that such persons have been cleared by the government at the appropriate level.

c. Utilization of Contractor to Accomplish Research, Development, or Production of COMSEC Information or Material. When in the best interests of the government, Heads of UA's may provide COMSEC material or information to a contractor for research, development, production, and testing of CRYPTO equipment, or of communications equipment interfacing with CRYPTO equipment, when such work is being undertaken on behalf of the government.

1-503 Subcontracting COMSEC Work.

a. Subcontracts requiring the disclosure of classified COMSEC information will be awarded only upon the written approval of the contracting officer of the prime contract. Prior to the approval of the subcontract, the contracting officer shall assure that the-proposed subcontractor meets the security requirements of this regulation.

b. The subcontractor facility shall be inspected in accordance with paragraphs 4-103 and 4-107.

1-504 Establishing a COMSEC Account.

a. When COMSEC material which is accountable to a COR is to be provided or produced under a contract, the contracting officer shall inform the contractor that a COMSEC account must be established. In addition, the contracting officer shall notify the COR and the CSO that a COMSEC account shall be established. The contractor is then required to nominate a COMSEC * custodian and an alternate COMSEC custodian, each of whom shall be a U.S. citizen.

b. The CSO shall forward the names of the persons nominated * as FSO, COMSEC custodian, and an alternate to the COR, with a copy to the contracting activity, indicating that the persons have been cleared and have been given a COMSEC briefing in accordance with paragraphs 2-313 and 2-314.

c. The COR will then establish the COMSEC account and will include the applicable contract number on each letter of transmittal or transmittal voucher sent to the contractor.

d. An individual may be appointed as the COMSEC custodian for more than one account only when approved by each COR concerned. ,

1-505 Destruction and Disposition of COMSEC Material. The COR will provide directions to the contractor when accountable COMSEC material is to be destroyed. These directions may be provided in superseding editions of publications or by specific instructions.

1-506 Shipment of COMSEC Material Outside of a Facility.

a. The contracting activity shall provide the contractor approval of and instructions pertaining to the shipment of classified COMSEC material. Methods for shipment are contained in reference (q).

b. If contractor personnel are to act as couriers to transport TOP SECRET keying material marked "CRYPTO," they must be designated by-the contracting activity. Such contractor personnel *must* be cleared for access to TOP SECRET material and must have been given a COMSEC briefing.

1-507 Unsolicited COMSEC Proposals. Any unsolicited COMSEC system, equipment, development, study, or proposal which is submitted by a contractor to a military department or an agency for consideration, shall be forwarded to the Assistant Director for Communications Security, National Security Agency, Fort George G. Meade, Maryland 20755, for evaluation and a determination as to whether or not it requires protection in the interest of national security.

Part 6. TRANSMISSION OF CLASSIFIED MATERIAL

1-600 Application. This part applies in those instances when, in accordance with paragraph 17, ISM, the contractor requires the approval of *or* instructions from the contracting activity for transmission of classified material outside the facility, and when CONFIDENTIAL material is transmitted to and from a contractor facility and a UA. *

1-601 Approved Methods of Transmission.

a. Approved methods for transmission of CONFIDENTIAL material *out*-side a contractor facility are set forth in paragraph 17d, ISM. That paragraph provides, in part, that contractors shall transmit CONFIDENTIAL material to other contractor facilities by U.S. Express Mail, U.S. Certified, or Registered Mail, depending on the contractors' location. . .

b. UA'S are not authorized to transmit CONFIDENTIAL material to a contractor facility by first class mail. Such material shall be transmitted only by U.S. Certified, U.S. Express or Registered Mail, in order to assure such transmission is received by an appropriately cleared employee of the contractor. *

c. In addition to the methods of transmission of classified material authorized in paragraph 17, ISM, contracting activities shall authorize additional methods when required in accordance with instructions contained in the

DAR and departmental or agency regulations. Further, when transmitting SECRET or CONFIDENTIAL material to an individual operating as a cleared facility or engaged as a Type B or Type C Consultant, or to any facility , at which only one employee is assigned, it shall specify on the outer container: "TO BE OPENED BY ADDRESSEE ONLY." The outer container shall also be annotated: "POSTMASTER -- DO NOT FORWARD. IF UNDELIVERABLE TO ADDRESSEE, RETURN TO SENDER. "

1-602 Contracting Officer Approval. Approval for or specific instruction to the contractor are required under the following conditions.

a. TOP SECRET material is to be transmitted outside a facility. The purpose of this requirement is to ensure that TOP SECRET information is not exposed to the inherent dangers of transmittal outside of the facility, unless essential to the performance of the contract.

b. The nature of the classified shipment does not lend itself to transmission by any of the methods specified in paragraph 17, ISM.

c. Use of Army, Navy, or Air Force postal facilities or Armed Forces Courier Service (ARFCOS) is required. However, such approval is not required provided that the contractor has previously received an authorization by virtue of his or her location on an overseas U.S. installation 14/. *

d. A CRYPTOSYSTEM Is to be used for the transmission of SECRET and CONFIDENTIAL information. Once approved and installed, the CRYPTOSYSTEM may be used for the transmission of such information pertaining to other classified contracts without further approval of the contracting activity concerned,. When- an urgent requirement exists for transmitting a considerable amount of information to and from the facility, and other methods of transmission are inexpedient, the contractor-may utilize the CRYPTOSYSTEM. TOP SECRET Information shall not be transmitted over a CRYPTOSYSTEM without the specific prior approval of *the* contracting officer concerned.

14/ If the intended recipient is not authorized to receive classified material through Army Post Office (APO) channels, arrangements shall be made with a U.S. activity which is so authorized to receive and hold the classified material pending pickup by the intended recipient. *

e. For transmissions which are not within or between the U. S., Puerto Rico, or a U.S. possession or a trust territory, but which are necessary to serve a government purpose, the contractor shall request written authorization from the contracting officer when the classified material is to be transmitted by one of the following means:

(1) by use of a cleared contractor employee escort who has been designated by the contractor, provided the transmission does not cross international boundaries, is accomplished (begun and completed) during normal daytime duty hours of the same day, and is in accordance with the agreements in effect with the country concerned;

(2) by use of cleared U.S. military personnel or civil service employee designated to escort shipment -- foreign carriers shall not be utilized except when the escort has continuous physical control of the material being transmitted;

(3) by use of U.S. and Canadian registered mail and via a U.S. . or Canadian government. activity; or

(4) when the transmission of U.S. classified information to a . foreign government is on a government-to-government basis (see paragraph 8-104).

On receipt of such request, the contracting activity shall verify the need for the shipment, determine that the procedures proposed by the contractor will provide a secure method of shipment, and assure that the shipment is destined for location where it can be stored under U.S. Government control or in the case of paragraph (4) above, it is under U.S. control until delivered to the representative of the foreign government. If the request meets the above requirements and is approved, the contracting activity shall so notify the contractor.

f. When shipment by truck is contemplated for classified CM (CONFIDENTIAL or SECRET), the contracting officer will issue specific shipping instructions, requiring a driver holding a final SECRET clearance in addition to the military escort normally provided for such shipments.

1-603 NATO Hand-carried Material. NATO regulations allow contractor employees to hand-carry NATO RESTRICTED, CONFIDENTIAL and SECRET. material across international borders under certain conditions. A contractor may request the CSO to approve the use of an appropriately cleared and briefed employee for such purposes in accordance with paragraph 88d, ISM. The CSO, after determining that the criteria for exception to normal transmission procedures exists, may issue an appropriately stamped and signed NATO Courier Certificate. The necessary formats are illustrated at appendix G, ISR and paragraph B, section III, attachment 3 to enclosure 2, of the USSAN Instruction 1-69, and will be originals on official letterhead. The CSO should affix an official seal to the certificate. If a NATO seal is not available, an official DIS or company seal may be used. During the course of recurring inspections, the CSO shall confirm that employees who are issued NATO Courier Certificates have been properly briefed and the certificates accounted for. The CSO will account for all courier certificates produced by them. (a consecutive numbering system should be devised by each CSO for this purpose.)

Part 7. PROCEDURES PERTAINING TO COMMERCIAL CARRIERS

1-700 Application. This part establishes procedures for the qualif icat ion of commercial carriers by both MTMC and DIS for the movement of SECRET controlled shipments. It specifics the responsibilities of MTMC in the CONUS and of designated military Commanders in' Alaska, Hawaii, Puerto Rico, and U.S. possessions and trust territories in their respective areas. It also specifies the responsibilities of CSO's assigned responsibility for assuring that commercial carriers can satisfactorily safeguard SECRET controlled shipments.

1-701 Instructions Concerning Commercial Carriers.

a. Requirements for the safeguarding of SECRET controlled shipments from consignor to consignee are established in the ISM and DoD 5220.22-C (reference-(b)). These-publications are distributed by the CSO's to cleared commercial carriers.

b. Appendix E reflects the areas serviced by MTMC and by military Commanders in Alaska, Hawaii, Puertc F.ice, or a U.S. possession or trust territory.

c. Appendix F is a chart which identifies the primary functional responsibilities of the transportation officer (TO), MTMC, and the CSO's, with respect to the transmission of SECRET controlled shipments by commercial carrier.

d. Annex A of reference (b) incorporates a *glossary of terms* applicable *to* commercial carrier procedures.

e. Transportation officers should refer to the "Military Traffic Management Regulation,'* reference (y), for transportation policies and procedures.

1-702 Approval of Commercial Carriers. Commercial carriers shall be qualified by MTMC to move SECRET controlled shipments for the DoD., other UA's, and government contractors when the movement of material is within the CONUS, or by the designated military Commander when the movement of material is wholly within Alaska, Hawaii, Puerto Rico, or a U.S. possession or trust territory. In addition, they must be cleared by the CSO. Requests for qualification of initial and additional carriers shall be submitted through channels to the appropriate MTMC area headquarters or the designated military Commander (see appendix l?) who shall maintain records of qualified commercial carriers and provide appropriate dissemination.

a. Qualification shall be based on the following.

(1) The requirement for the carrier's service has been established by a shipper.

(2) A determination has been made by MTMC or designated Commander that a qualified and cleared carrier is not available to perform the required service. In this connection, MTMC or the designated Commander shall

coordinate with the Deputy Director (Industrial Security), HQ DIS to ensure that a cleared carrier is not available.

(3) The carrier is authorized by law, regulatory body, or regulative to provide the required transportation service.

(4) A determination has been made by MTMC or designated Commander that the carrier is capable of, and authorized to, furnish PSS by applicable tariff, government tender, agreement, or contract provision, as required by paragraph b below.

(5) The carrier has been granted a SECRET FCL by the CSO.

b. The commercial carrier, by applicable tariff, government tender, agreement, or contract provision agrees to provide the following protective services for the movement of SECRET controlled shipments.

(1) The commercial carrier agrees to provide continuous person-to-person tally and signature of those persons providing en route protection while the shipment is in the carrier' a custody; for air shipments, which are loaded into a compartment which is not accessible in flight , no receipt will be required from the flight crew or attendants of the carrier's aircraft on which shipments are being transported.

(2) The commercial carrier agrees to provide constant protection of the shipment at all times, between receipt from the consignor until delivery to consignee, by one or more cleared employees to prevent inspection, tampering, or pilferage. Observation of the shipment is not required during the period it is stored in the carrier's aircraft, in connection with flight, provided the shipment is loaded into a compartment aboard the aircraft which is not accessible to any unauthorized person.

(3) Closed and locked compartments or vehicles shall be used for shipment except when another method is authorized specifically by the shipper. In any event, exception shall not be granted for individual packages weighing less than 200 pounds gross.

(4) Shipments normally shall be afforded single-line service from point of origin to destination when such service is available. If time or distance does not permit movement through, the following security procedures will be observed.

(a) If the shipment remains in the transportation equipment, at least one of the cleared carrier custodians shall maintain constant protection to prevent access to shipment by unauthorized persons.

(b) If the material is unloaded from the vehicle, it shall be under the constant protection of a carrier custodian at the storage site or shall be placed in storage in a closed area., vault, or strongroom as defined in the ISM.

(c) In those cases in which the shipment is placed in storage en route, one of the cleared carrier custodians of the storage site shall execute the tally **and signature service, and assume appropriate protection as prescribed.**

c. The MTMC or the designated military Commander shall request the CSO of the commercial carrier's **HOF to** process the carrier and identified terminals for a FCL following completion of the actions prescribed **in** paragraphs a(l), **(2),** *(3),* and (4) above. Prior coordination with the **Deputy** Director (Industrial Security), HQ DIS will be made to determine the specific terminals to be processed for clearance. On receipt of a request for qualification, **the CSO** concerned **shall** complete the actions prescribed **in** section II, part 1 to permit an administrative determination to grant or deny a FCL to the carrier. **During** the initial survey, the **CSO** will assure that the contractor **is** *aware* that preparation **of an** acceptable SPP **is** a prerequisite **to** granting a **FCL** and that only those terminals listed **by the HOF** on the "Appendage **to** the Transportation Security Agreement" (DIS Form **1150)** may be used for SECRET controlled shipments.

i-703 Responsibilities of Cognizant Security Offices. In addition to **those** actions prescribed in paragraph 1-702, **CSO's assigned responsibility** under paragraphs **1-300f** and **1-300g** of this section, shall be responsible for the **following.**

a. Inspect the HOF and the specific terminals of the carrier authorized to handle **SECRET** controlled shipments in **accordance** with **the** schedule in paragraph 4-103. The purpose of this inspection is to ensure that the carrier is complying with the **terms** of the "DoD Transportation Security Agreement" **(DIS** Form 1149), reference (b), and the carrier's SPP, Indications of noncompliance **requiring** ore frequent or extensive types of inspection are not limited to those derived from inspections, but may be obtained from any reasonable source including complaints and prescribed reports submitted by any cleared contractor or government agency using this service.

b. Conduct appropriate inquiries into the circumstances involving **delay** in the movement of SECRET controlled shipments by commercial carriers, violation, or the possible loss of security due to **misrouting,** loss, tampering, or emergencies.

c. Advise the carrier's management **of all** deficiencies and of the requirement for corrective action **in** each case. Necessary follow-up inspections **shall be** performed **by CSO's** to determine the completion and effectiveness of corrective actions required of the carrier.

d. Ensure that the appropriate government investigative agency *is* advised of reports **received** by the CSO concerning existing or threatened espionage, sabotage, or subversive activities.

e. Advise carrier management concerning their obligations under the **provisions** of the DIS *Form* 1149, **"Department** of Defense Transportation Security Agreement," May 1983 (reference (old)) and reference (b).

f. Determine the effectiveness of the carrier in protecting SECRET controlled shipments. *If* the carrier's ***performance*** is determined to be

unsatisfactory and cited discrepancies are not corrected within a reasonable period of time, the CSO shall take the action prescribed in paragraph 4-202. In order to provide for an adequate review of the effectiveness of a carrier's performance, all involved government or contractor activities shall furnish copies of all reports or incidents, investigations, inspections, surveys, or other documents which reflect unsatisfactory performance in the protection or movement of SECRET controlled shipments by a commercial carrier to the responsible CSO.